DOI:10.13811/j.cnki.eer.2009.09.029

[文章编号]1003-1553(2009)09-0070-04

高等教育信息化发展中的几个热点问题研究

——网络安全与信息管理

李 华

(西北师范大学 教育技术与传播学院，甘肃 兰州 730070)

[摘 要] 随着我国高等教育信息化的深化发展及 Internet 的普及，信息化网络技术已经深入渗透到高等学校教育教学的各个方面，教育管理者、科研工作者、教师及莘莘学子们享受信息化校园网络带来方便的同时，网络安全、信息安全问题也日益突出。本文就目前我国高等教育信息化发展中的网络安全与信息管理问题进行研究，结合当前高等教育信息化深化发展的实际，在问题分析的基础上，提出了一些问题解决的建议与对策。

[关键词] 高等教育；信息化发展；网络安全；信息管理

[中图分类号] G434 [文献标识码] A

一、网络安全问题的提出

信息化校园网络作为高等教育信息化的基础设施，其安全运行状况直接关系到高等教育信息化的发展进程。

信息安全问题最早是从通信安全问题开始的。此后，随着计算机网络技术的发展及网络的普及应用又提出了“网络安全”。网络安全问题的提出，源于计算机病毒的出现。1983 年，弗雷德·科恩博士编写了一种在计算机运行过程中可以复制自身的破坏性程序，伦·艾德勒曼将它命名为 “计算机病毒”，“计算机病毒”一词由此诞生。在计算机病毒史上，具有重要里程碑意义的是震惊世界让网络瘫痪的蠕虫病毒。这种具有主动攻击特征的网络蠕虫一出现就成功地攻击了美国国防、军事科研单位与有关大专院校联入互联网的 6000 余台计算机（占当时互联网联机的 1/10 左右），使其瘫痪。导致当时的美国总统里根签署了《计算机安全法令》。据美国 FBI 统计，美国每年因网络安全问题所造成的经济损失高达 100 多亿美元，还有日益增加的趋势.另据有关部门统计，在所有的计算机安全事件中，约有 52%是人为因素造成的，25%由火灾、水灾等自然灾害引起，技术错误只占 10%，组织内部人员作案占 10%，仅有 3%左右是由外部不法人员的攻击造成。由此可以看出，属于管理方面的原因比重占到 70%以上，也就是说，真正的信息安全是需要系统科学有效的管理来保证。

二、当前高校信息化校园网络安全问题

(一)高校信息化校园网络的环境安全问题

从物理环境角度来看，高等学校校园网依然经受着诸如盗窃、火灾等环境因素的困扰，尤其是近年来高校信息化校园网络设备的普及应用，校园计算机设备成了高校内偷盗者的重要目标，偷窃者从以往的整机盗窃，发展到只盗内部心脏，如 CPU、主板、内存条、光驱、硬盘等高价值的东西。有时计算机偷窃行为所造成的损失可能远远超过计算机本身的价值。静电、雷击、电磁泄漏等环境因素更不可轻视，强静电若未能及时释放而保留在设备内，会形成很高的瞬时电位，一旦产生静电放电，轻者会使大规模集成电器损坏，重者造成机器自燃爆炸，甚至引发火灾。雷击尤其是感应雷更是电子信息设备受损的主要杀手。电磁泄漏是电子设备本身所特有的现象，计算机在工作时会产生电磁发射，这种电磁发射有可能被高灵敏度的接收设备所接收，造成计算机信息泄露。对于高度保密工作的计算机网络，电磁泄漏是不可被忽视的安全问题。

(二)高校信息化校园网络的自身安全问题

当前对高校信息化校园网络安全构成的威胁除环境因素外，更多的校园网络的安全问题来源于网络本身。它既包括信息化校园网络系统本身的脆弱性和潜在威胁，也涉及管理方法和人为因素，以及来自外

部的攻击。这主要体现在以下几个方面:

1. 系统自身存在的安全隐患和安全漏洞

互联网的开放和普及,网络应用与信息通信频繁,由于网络系统自身存在的安全隐患和安全漏洞,会使一些不怀好意的人有机会通过互联网对数字化校园网络信息进行窃听、截取或篡改等方式的攻击。目前很多软件(包括网络协议、操作系统、应用软件等)存在诸多漏洞,加大了数字化校园网络系统被攻击的可能性,如一些专门针对操作系统自身漏洞的计算机病毒程序会使系统容易受到攻击。有名的 Windows DCOM 蠕虫病毒就是利用 Windows 漏洞进行攻击的。

2. 网络非法入侵者的攻击

在互联网上,一些攻击网络的工具的出现,由于获取容易、使用简便,致使网络受攻击的复杂程度在不断降低,一个普通的攻击者也可以对系统造成巨大的危害。有些精通计算机的学生,由于其强烈的猎奇心理而成为网络黑客,冒充合法用户,对网络设备及信息资源进行非正常使用和越权使用,或者利用假冒和欺骗的手段非法获得用户的使用权限,以达到占用资源的目的。而一些恶意的网络黑客则使用非法手段删除、修改、重发某些重要信息,影响用户的正常工作。校园网与互联网相连,高校校园网中教学、科研和行政办公的电脑中存有涉及机密的文件,如招生信息、学生成绩档案资料、学校财务状况以及教师的一些个人信息、高科技研究成果等,都是网络黑客觊觎的目标。每天都会有入侵者试图闯入网络节点,利用这些主机在管理上的松懈来达到发动攻击的目的。

3. 网络病毒的侵害

网络病毒与恶意攻击主要是通过互联网络传播病毒或恶意脚本文件等,干扰用户的正常使用。高校信息化校园网络中网络病毒或木马程序主要通过以下途径入侵:一是电子邮件,二是从网络上下载资料时,三是盗版软件,四是 Internet 上一些恶意网站或垃圾邮件,五是带有病毒的移动存储设备等。其危害特征表现在冻结机器的注册表、更改 IE 设置等,造成系统的不稳定,使校园网用户的计算机无法正常工作。

4. 校园网用户的安全意识薄弱

当前校园网用户对网络安全尚未能充分认识,对所使用计算机应作安全防范很多都不到位。校园网用户更多地侧重于各类应用软件的操作上面,以期望方便、快捷、高效地使用网络,最大限度地获取有效的信息资源,而很少考虑实际存在的风险和低效率,很少学习防范病毒、漏洞修复、密码管理、信息保密的必备知识以及防止人为破坏系统和篡改敏感数据的有关技术。比如许多教师为了办公方便,将所有硬盘分区共享,并且不限制权限,使其他用户通过网上邻居等简单方式就可以对文件进行操作,为入侵者提供可乘之机。

5. 网内的人为安全隐患

校园网内部存在的安全隐患主要来自于人为因素。具体体现在以下三个方面:第一,管理人员操作失误造成的安全隐患。如管理人员在新设用户账户、修改用户账户及进行其他日常维护任务时,无意中把管理权限授给了不合适的用户,用户不经意获得了不应该拥有的权限。这些新授权的用户无意中给数据和系统带来破坏。第二,人为蓄意破坏带来的安全隐患。如一些学生利用系统可能存在的漏洞及对用户和用户组权限管理不善,进行蓄意攻击。还有的设立特洛伊木马以获得访问权,在校外非法访问极为重要的信息内容。第三,学生的无知所引起的安全问题。现在很多大学生的计算机技术水平非常高,但网络安全意识、安全法规淡薄。他们时常会有意无意地破译密码进入校园网核心层。有的人编制一些程序来试探网络系统的安全性而形成网络病毒,干扰校园网安全正常运行。更多的是一些学生的无知,在系统设置中无意地造成了网络系统的安全漏洞。总之,来自校园网内部的安全隐患比来自校园网外部的各种不安全因素破坏力更强、影响更广、威胁更大,因为对于这些来自于防火墙内的人为因素,入侵检测系统或抗病毒软件对此都是无能为力的。

三、高校信息化校园网络安全对策及信息安全管理

(一)物理层面的安全管理对策

物理层面的安全管理策略其目的是在物理层面上保护信息化校园网络系统,如计算机系统、网络服务器等硬件实体和通信链路免受自然灾害、人为破坏和搭线攻击。建构信息化校园网时要充分考虑到学校所在地环境、气候条件、抗干扰能力等多方面的因素。对网络布局、设备选型、安装配置等进行统一规划和分析论证,对防盗、防火、防静电、防雷击、防电磁泄漏措施也都要预先进行设计。体现在具体管理上,第一,建立完备的安全管理制度,防止他人非法进入信息化场所,安全用电和严禁吸烟是信息化网络场所防火、防盗最基本的安全管理要求;第二,信息化网络机房要安装防静电设施,确保计算机系统有一个良好的电磁兼容工作环境;第三,构建科学有效的防雷系统,根据电气、微电子设备的不同功能及不同受保护程序和所属保护层,确定防护要点作分类保护。根据雷电和操作瞬间过电压危害的可能通道,从电源线到数据通信线路作多级

层保护;第四,重要核心机密机房要设计抑制和防止电磁泄露的屏蔽装置,有效防止信息泄漏。

(二)网络层面的安全管理措施

网络安全管理的核心是要保证网络信息数据的保密性、完整性、可靠性及可用性。网络的安全管理在技术层面所要采取的措施:第一,网络访问中的权限控制。通过入网访问控制、网络权限控制及客户端安全保护策略等措施,验证用户的身份和使用权限,防止用户越权操作,来保证网络资源不被非法使用和非法访问,达到网络的访问控制安全。第二,信息传输中的加密处理。网络上的任何信息都要经过重重中介分段传送到目的地。网络信息的传输是无固定传输路径的,因此任何中间节点均可能拦截、读取甚至破坏和篡改封包的信息,并且难以查证。信息传输安全问题不可轻视,利用加密技术确保信息传输的安全是最有效的方法。所以我们在用网络传输重要的信息时,一定要对信息进行加密技术处理。第三,用口令字、文件许可等保证计算机的逻辑安全。第四,通过"防火墙"技术阻隔入侵者,即时下载安装补丁程序修复系统漏洞等,保证操作系统安全。第五,要科学合理地配置网络服务器,减少因配置错误而产生服务器安全漏洞。服务器配置中留下的漏洞可以使入侵者获取系统的最高控制权。因此,网络服务器安全的保证需要有高素质高技术能力的管理人员来管理维护。

(三)有效的信息安全管理措施

在高等教育信息化建设过程中,不少高校把精力放在了网络硬件和应用建设方面,而忽视网络的安全与管理。要保障校园网络的信息安全运行,更多的是要靠网络安全意识、网络安全技术、安全管理制度和科学的管理。

1. 加强校园网用户的信息安全意识教育

当前高校信息化建设中,信息安全教育是一个薄弱环节,加强对教师学生的网络安全意识教育非常必要。第一,大力宣传、宣讲网络信息安全知识、网络安全管理制度,让师生认识到信息时代网络安全的重要性,自觉遵守网络安全管理制度。第二,通过普及网络安全知识,利用课堂、讲堂、网络平台让师生学习防范病毒、漏洞修复、密码管理、信息保密的必备知识,提高师生的网络安全管理技术水平。第三,开设相关课程,提高学生的网络修养,要有法律意识,遵守网络安全法规,自觉抵制网络不良信息和反动信息,不随意乱发帖子和不良信息,不充当网络黑客,做一个遵纪守法的好网民。

2. 建立健全信息安全管理制度

高等学校的信息安全首要的是要制定一系列完整规范的信息安全管理制度,并贯彻执行,使得管理者和应用者从思想上、意识上、行动上高度重视信息安全的重要性,将网络内部的信息安全隐患减少到最低。信息安全管理制度除国家制定的相关法律、法规外,还要根据自己学校的实际制定相关的安全管理制度,如管理员网络维护管理制度、服务器机房出入管理制度、外来人员网络访问制度等。约束普通用户等网络访问者,督促管理员很好地完成自身的工作,增强大家的网络安全意识,防止因粗心大意或不贯彻制度而导致安全事故。尤其要注意制度的监督贯彻执行。

3. 重视信息安全管理技术人才培养

信息安全管理的技术保障包括技术人才、安全方案和技术处理等内容。其中技术人才是技术安全保障的根本,要重视培养专业的网络安全管理技术人才,提高网络安全管理技术人员的能力水平。安全方案是整个系统安全保障的根据,安全方案涉及到安全理论、安全产品、网络技术、系统技术实现等多方面专业技能,对网络安全管理人员能力要求较高,对于那些不具备此能力的,可以聘请专业安全顾问来协助完成。高等学校的信息安全管理主要依靠自己的力量来完成技术支持保障,因此,要重视加强网络管理人才的培养,让管理技术人员接受良好的安全管理培训,具有快速的安全事件响应的能力,能够有效解决网络的安全问题。

4. 建立信息安全管理的安全保障体系

建立完善的安全保障体系是系统安全所必需的。管理人员的安全培训、可靠的数据备份、紧急事件的响应措施、定期系统安全评估及更新升级系统,这些将会为系统的安全提供有力的保障,确保系统能一直处于最佳的安全状态,即便系统受到攻击,也能最大程度地挽回损失。高等学校中学生的档案信息、教务管理信息、图书情报信息、知识创新与科研成果信息等重要信息,都要有高水平的管理人员来管理,一些重要的信息需要可靠的数据备份,如数字图书情报资源信息可以通过搭建信息存储架构、将整合集中在单一或少数系统平台架构上的数据和信息进行备份存储来管理。

四、结束语

随着计算机网络技术的更加广泛、普及,高校信息化校园中的信息化网络愈益成为师生获取信息、交流信息、学习知识和科学研究的强有力辅助工具。而且,高等教育信息化发展中网络安全与信息管理是一个

动态的且不断随技术进步而变化发展的问题。本文的研究通过对网络安全的起因、网络安全问题的成因的分析,提出了一些信息化校园网络安全的基本对策及信息安全管理的基本措施,以期对信息化校园网络的健康运行有益。当然,我们的研究只是冰山一角,也只提出了自己的一点粗浅的看法和观点,对于当前信息保密和系统安全做得并不十分完备的校园的网络安全问题还有待更多的人关注、研究。

[参考文献]

[1] 张志强,郝志萍.校园网络安全现状与安全策略构建[J].中州大学学报,2008,(3).

[2] 周扬玲.校园网安全问题及防范策略[J].四川职业技术学院学报,2008,(3):61~62.

[3] 张玉珍.高校知识创新中的信息保障体系研究[J].情报杂志,2005,(1):132~134.

[4] 钟平.试论数字化校园建设中对校园网络安全的要求[J].福建电脑,2008,(1):43.

(上接第 55 页)

内容,以及在协作学习中资料贡献情况,提问内容和次数及心得体会等,这些记录都是对学生进行教学评价的依据。

"计算机文化基础"这门课程采用了混合式的教学评价方式,学生的成绩由三部分组成,分别是期末考试成绩、教学系统中的成绩册成绩和电子档案袋评价工具中的学生作品成绩。其中期末考试成绩占总成绩的 30%、成绩册成绩占总成绩的 30%、学生作品成绩占总成绩的 40%,突出考核学生的实际动手操作能力。与传统的教学评价方式相比,采用混合式教学评价更能考核出学生的真正水平,避免了传统考试中重成绩、轻能力的情况发生。

四、结束语

通过"计算机文化基础"课程在 Sakai 教学系统中一个学期的实施,可以看到,与传统教学方式相比,在注重应用和操作性的课程中实施混合式教学,既可以保证教师主导作用的发挥,也有利于激发学生的学习兴趣,提高学习的积极性,对培养学生的创新精神、自我设计能力和自主学习意识都有积极作用;Sakai 教学系统零成本、教学功能齐全、可以根据需要添加课程管理工具,受到师生的一致欢迎,证明其可以作为一个通用的教学支撑平台来使用。

[参考文献]

[1] 何克抗.从 Blending Learning 看教育技术理论的新发展[J].国家教育行政学院学报,2005.(9):37~48.

[2] 田富鹏,焦道利.信息化环境下高校混合教学模式的实践探索[J].电化教育研究,2005,(4):63~65.

[3] J. Farmer. Interoperability: A Community Aspiration[Z]. Sakai Project, University of Michigan,2004.

[4] Anthony Whyte.Sakai Tool List (2.5) [EB/OL].http://confluence.sakaiproject.org/confluence/display./DOC/Tool+List+%282.5%29,2008—6—23.

[5] 朱莹莹,胡航. Sakai:教育中的合作与学习环境[J].中国教育信息化,2008,(3):16~19.

[6] 陈声健.高校混合式学习教学设计的研究[D].北京师范大学,2006.